PRV ●

PATENT- OCH REGISTRERINGSVERKET
Patentavdelningen

Intyg
Certificate

Härmed intygas att bifogade kopior överensstämmer med de handlingar som ursprungligen ingivits till Patent- och registreringsverket i nedannämnda ansökan.

This is to certify that the annexed is a true copy of the documents as originally filed with the Patent- and Registration Office in connection with the following patent application.

(71) *Sökande*   ABB AS, Billingstad NO
    Applicant (s)

(21) *Patentansökningsnummer*   0203819-8
    Patent application number

(86) *Ingivningsdatum*   2002-12-19
    Date of filing

Stockholm, 2004-03-22

För Patent- och registreringsverket
For the Patent- and Registration Office

Hjördis Segerlund

Avgift
Fee   170:-

2002-12-17
9498SE-LG

Method to increase the safety integrity level of a control system

TECHNICAL FIELD.

The present invention relates to supervision, diagnostic and diversity of execution of control algorithms in the context of control systems. A device comprises functionality, which adds security features to a controller and enables the controller to meet requirements for a safety control system. Such a system needs diagnostic in order to ensure that no accidents take place which otherwise could harm people, equipment or the environment.

BACKGROUND ART.

Industrial control systems are for instance applied in manufacturing and process industries, such as chemical plants, oil production plants, refineries, pulp and paper mills, steel mills and automated factories. Industrial control systems are also widely used within the power industry. Such industrial control systems may need to comprise or be combined with devices, which adds safety features. Example of processes which requires additional safety features than what a standard industrial control system provides are processes at off-shore production platforms, certain process sections at nuclear power plants and hazardous areas at chemical plants. Safety features may be used in conjunction with safety shutdown, fire and/or alarm systems as well as for fire-and-gas detection.

The use of advanced computer systems in safety related Huvu...en Kossan
control systems raises challenges in the verification of
correctness of large amount of software code and the
complex electronics. There exist prior art, for instance

5   described as standards, for how higher safety level can
be obtained for such systems. Such prior art is commonly
focused on the process of the development of products
both the hardware part and the software parts. It also
describes diagnostic functionalities and algorithms.

10   Prior art also address the higher safety level obtained
in executing control systems with different hardware
redundancy and software diversity. The implementation of
an advanced safety control system is normally based on a
dual or triple system with some type of voting before

15   enabling an output signal. Some safety control systems
have implemented a sufficiently safe single unit solution
by focusing on design of the system and highest possible
quality in implementing such system. Both multiple unit
systems and single unit systems have today often included

20   some number of diagnostic algorithms both in software and
in hardware.

An example of an industrial control system, which
includes a safety critical function, is described in

25   DE19857683 "Safety critical function monitoring of
control systems for process control applications has
separate unit". The system has a main controller bus
coupled to different processors via a number of
decentralized data receivers.

30

One example of a device in an industrial control system
which has increased capability of fault detection is
described in GB2277814, which concerns a fault tolerant
PLC (Programmable Logic Controller) including a Central

Programmable Unit (CPU). A pair of first I/O modules are
connected between a positive power bus and a load. A pair
of second I/O modules are connected between the negative
power bus and the load. GB 2 277 814 further describes

5 . that power to the load is not disconnected upon failure
of one of the I/O modules on either side of the load.

US 6,201,997 describes a two-processor solution where
both processors receives the same input data and

10 processes the same program.

SUMMARY OF THE INVENTION
The object of the invention is to enable an increased
safety integrity level of a Control System.

15

This object is met by a method to increase a safety
integrity level of a Controller for control of real world
objects, the steps attaching a safety hardware unit,
downloading software to a CPU of the Controller and the

20 attached safety hardware unit, configuring the attached
safety hardware unit to set the Controller's output
values in a safe state for on-line control.

An advantage with the invention is that it increases the

25 safety level for a control system based on a single
controller unit to a level, which previously was
available mainly for dual or triple controller systems.
The invention reduces the complexity of implementing and
maintaining such control systems.

30

Another advantage with the invention is that a control
system based on the invention and qualified for a high
safety level control may also be used for non-safety
critical process control by not using the added safety

hardware unit. The invention enables an increased
flexibility in the use of the single unit controller.
This process control use of the single controller will
then be a less costly and faster controller then the full

5   safety level use of the control system. Since the plug-
able safety hardware unit is not used for non-safety
critical control, a smaller amount of software in the
single controller, compared with prior art, allows larger
application software to execute faster.

10

Another advantage with the invention is that it enables
that a Controller may reach an increased safety integrity
level at a time after that the Controller was originally
installed for control of real world objects. As an

15   example a Controller may first be installed to perform
non-safety critical control and a year later the
Controller is configured for an increased safety
integrity level for safety critical control.

20   An additional advantage is the solutions obtained on how
the user interfaces the plug-able unit. The user
interface will be simplified to that for instance an
engineer will specifies the wanted level of safety
integrity for the application.

25

Another object of the invention is to provide a Control
System intended for safety related control of real world
objects. The control system comprises a Controller with a
single main CPU, and an attached safety hardware unit

30   comprising means to increase the safety integrity level
of the Control System.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will be described in more detail in connection with the enclosed schematic drawings.

Figure 1 shows an overview of a method according to the
5   invention.

Figure 2 shows a simplified diagram of a Controller with a local Input/Output and with an attached safety hardware unit.

10

Figure 3 shows a simplified diagram of the Controller with an attached safety hardware unit with remote Input/Output connected by a bus solution.

15   Figure 4 shows an overview of a Control System comprising a Controller with an attached safety hardware unit.

DESCRIPTION OF THE PREFERRED EMBODIMENTS
Figure 1 shows an overview of a method according to the
20   invention. The method provides an increased safety integrity level of a Controller 10 such as an Industrial Controller of an Industrial Control System. Examples of a Controller is a Programmable Logical Controller (PLC) and a field controller.

25

In this description a Controller has the purpose of collecting measurements and controlling real world objects connected to a Control System. Examples of real world objects are valves, motors, pumps, compressors,
30   switchgears, conveyor belts, a product, a raw material or a batch.

With safety integrity level is meant a controller which meats de-facto standard safety integrity levels or

standard safety integrity levels, such as SIL 1, SIL 2,
SIL 3 or SIL 4 (SIL according to the standard IEC 61508
or later IEC standards).

5   Figure 1 shows that the method comprises a step of
    attaching 1 a safety hardware unit 11 (shown in Figure 2)
    to the Controller 10. The safety hardware unit 11
    communicates with the Controller's CPU. The safety
    hardware unit 11 may be in the form of a circuit board
10 and typically comprise a CPU and may also comprise an
    Input/Output (I/O) interface. Such an I/O interface may
    comprise a set of memory chips and a Field Programmable
    Gate Array (FPGA). The Safety Hardware Unit may also
    comprise local I/O channels such as Digital Output (DO)
15 in order to provide forced output signals for instance to
    an external alarm system. Further, the Safety Hardware
    Unit may include functionality for memory shadowing. One
    alternative name for the safety hardware unit 11 is a
    safety module. The safety hardware unit 11 comprise
20 communication means to communicate with the Controller's
    CPU via a bus 14. The safety hardware unit 11 may be
    connected via a back-plane to the Controller 10. In an
    alternative embodiment the safety hardware unit 11 is a
    plug-able unit added to the main circuit board of the
25 Controller 10, comprising the main CPU of the Controller
    10.

    Further, figure 1 shows that the method comprises the
    step of downloading software with safety related
30 configuration data, not only to the Controller 10 shown
    in figure 2, but also to the attached safety hardware
    unit 11. In one embodiment the downloading of such
    software is made from a software tool connected to the
    Controller 10 from a computer device, such as a Personal

Computer or Workstation. An example of configuration data
is application classification depending on the previously
mentioned safety standard. Configuration of communication
capabilities between safety related applications. Other
5   examples of such configuration data are application
access level, which relates to user-authorization
control.

Another step of the method, shown in figure 1, is
10 configuring the safety hardware unit 11 to execute safety
function logic and set the Controller's 10 output values
into a safe state for on-line safety control. This
insures that the Control System 20, shown in figure 4,
goes into a safe-state. To set the output values into a
15 safe state is either made in an active way or in a
passive way. The execution of the safety function logic
depends on the configuration data. The safety function
logic is written in a language well known to a person
skilled in the art. Such a language may be according to
20 IEC 6-1131 with possible extensions for safety related
functions.

The Controller 10 has the same control functionality for
non-safety related control both with and without the
25 attached hardware unit 11. It should be appreciated that
compared with prior art this enables more flexible
technical solutions for safety control. As an example the
Controller 10 has the same set of program instructions
available both with and without the attached hardware
30 unit 11. An example of a program language is structured
text as defined by IEC 6-1131. This means that a
Controller 10, which originally is configured only for a
non-safety critical application, may at a later time be
configured with the safety hardware unit 11 mentioned

above, and after being configured for on-line safety
control the Controller 10 may still run the same non-
safety critical application as before adding the safety
hardware unit 11.

5

In an embodiment of the invention a controller
configuration and controller code is downloaded to the
Controller 10. It is a user 22 of a software tool that
initiates a download of the controller configuration and

10   controller code. An example of a user is a process
engineer, a service engineer or a process operator.
During or after that controller configuration and
controller code is defined a hardware unit diagnostic
information is generated. In the embodiment the

15   diagnostic information is down-loaded to the attached
safety hardware unit 11 and is intended for on-line
diagnostic purposes.

Figure 2 shows that a Controller referred to in the above

20   described method, shown in figure 1, may obtain access to
a plurality of input and output unit directly connected
to the Controller.

Figure 3 shows that a Controller referred to in the above

25   described method, shown in figure 1, may obtain access to
a plurality of input and output values of a real world
object through a bus connected between the Controller and
to an input/output unit. In such an embodiment the
validity of the bus communication is verified in the

30   attached safety hardware unit 11. An example of such an
input/output unit is a remote I/O. An example of a bus is
a fieldbus. Another example of a bus is an internal bus
of the Controller, such as a bus running on the backplane
of the Controller 10.

It is an advantage if the bus verification logic is
implemented in diverse. Further it is an advantage if in
an embodiment of the invention the attached safety
5   hardware unit is diverse generating a safety related
header for the bus communication.

In order to further improve the reliability and
diagnostics of the Control System the Input/Output unit
10   15 may comprise two diverse implementations each
verifying the correctness of the bus traffic and each
generating a safety related header for the bus 14
communication.

15   Further in an embodiment of the invention the timing
supervision of the Controller 10 is verified in the
attached safety hardware unit 11. An embodiment of the
invention may also comprise that the correct sequence of
logic is verified in the attached hardware unit 11.
20   Further an embodiment may comprise that the correct
download of new control functionality logic is verified
in the attached hardware unit 11. Such a verification may
for instance involve a test of a check-sum.

25   It is beneficial to allow only users logged on as safety
classified users to modify the control functionality
logic and parameters. Such a classification may be
verified in the Control System by means of a user key.

30   The safety hardware unit 11 may be configured to run as a
slave of the Controller 10. That means that a safety
function logic executing in the safety hardware unit is
triggered from the Controller. The safety hardware unit
supervise that that it is triggered at a defined time.

In another embodiment the safety hardware unit 11 may
comprise a first and a second module in a redundant
configuration. The second module is typically updated
5   with data from the first module and the second module
takes over the safety related control of the control
system from the first module if a failure of the first
module is detected. The Controller may have a redundant
CPU unit, which takes over control of real world objects
10   from the primary CPU unit in the case of a failure of the
primary CPU unit. The redundant CPU establishes
communication with the first or second module of the
attached safety hardware unit.

15   Another embodiment of the invention is a Control System
20 intended for safety related control of real world
objects. Such a Control System comprise a Controller 10
with a single main CPU and an attached safety hardware
unit 11 comprising means to set the Controller's output
20   values in a safe state for on-line safety control.

CLAIMS

1. A method to increase a safety integrity level of a
Controller (10) for control of real world objects,
5   characterized by the steps of
- attaching to the said Controller (10) a safety hardware
unit (11) wherein the safety hardware unit (11)
communicates with the said Controller's CPU,
- downloading software with safety related configuration
10   data to the attached safety hardware unit (11) and to the
Controller (10),
- configuring the attached safety hardware unit (11) to
execute safety function logic, which depends on the
safety related configuration data, and in an active or
15   passive way set the Controller's (10) output values to a
safe state for on-line safety control.

2. A method according to claim 1, characterized in that
the Controller (10) have the capability of executing a
20   set of non-safety critical control functions, which set
of non-safety critical control functions is the same
before as well as after the safety hardware unit (11) is
attached.

25   3. A method according to claim 2, characterized in that
the configuring step comprise the additional steps of
- downloading to the attached safety hardware unit (11)
diagnostic information, which previously was
automatically generated by a software tool as a result of
30   user's configuration of the Controller (10) and which
diagnostic information is used in the attached safety
hardware unit (11) during safety critical control.

4. A method according to any previous claim,
35   characterized in that access to a plurality of input and
output values of a real world object is obtained through
a bus (14) connected between the Controller (10) and to

an input/output unit (15) and the validity of the bus
(14) communication is verified in the attached safety
hardware unit (11).

5   5. A method according to any previous claim,
characterized in that the timing supervision of the
Controller (10) is verified in the attached safety
hardware unit (11).

10   6. A method according to any previous claim,
characterized in that correct sequence of code logic is
verified in the attached safety hardware unit (11).

7. A method according to any previous claim,
15   characterized in that correctness of memory content of
the controller (10) is verified in the attached safety
hardware unit (11).

8. A method according to any previous claim,
20   characterized in that a download of new control
functionality logic to the Controller is verified in the
attached safety hardware unit (11).

9. A method according to any previous claim,
25   characterized in that the attached safety hardware unit
(11) performs checks in order to allow only users logged
on as safety classified engineers and safety classified
operators to modify the control functionality logic and
parameters.

30

10. A method according to claim 4, characterized in that
the bus (14) communication verification logic in the
attached safety hardware unit (11) is implemented
diverse.

35

11. A method according to claim 4, **characterized** in that
the attached safety hardware unit 11 is diverse
generating a safety related header for the bus (14)
communication.

5

12. A method according to claim 11, **characterized** in that
the Input/Output unit (15) has two diverse
implementations each verifying the correctness of the bus
(14) traffic and each generating a safety related header

10 for the bus communication.

13. A method according to any previous claim,
characterized in that the attached safety hardware unit
comprise a first and a second module in a redundant

15 configuration, the second module is updated with data
that exists in the first module at the time of a failure
and the second module takes over the safety related
control of the control system from the first module if a
failure of the first module is detected.

20

14. A method according to claim 13, **characterized** in that
the a redundant Controller unit is attached to the
Controller (10), which takes over in case of a failure of
a primary Controller and the redundant Controller unit

25 establish communication with either the active first
module or the active second module of the attached safety
hardware unit.

15. A Control System (20) intended for safety related

30 control of real world objects, **characterized** in that it
comprises
- a single main CPU handling the main processes of a
Controller (10),

- an attached safety hardware unit (11) comprising means
to increase the safety integrity level of the Controller
and the comprising means to set the Controller's output
values in a safe state for on-line safety control.

5

16. A Control System according to claim 15, characterized
in that the Controller (10) have the capability of
executing a set of non-safety critical control functions,
which set of non-safety critical control functions is the
10   same before as well as after the safety hardware unit is
attached.

17. A Control System according to claim 16, characterized
in that it comprises,
15   - means for downloading to the attached safety hardware
unit diagnostic information, which previously was
automatically generated by a software tool as a result of
user's configuration of the Controller and which
diagnostic information is used in the attached safety
20   hardware unit during safety critical control.

18. A Control System according to claim 17, characterized
in that it comprises
- an input/output unit (15) connected to the Controller
25   (10) by a bus and the validity of the bus (14)
communication is verified in the attached safety hardware
unit.

19. A Control System according to claim 18, characterized
30   in that the bus (14) communication verification logic in
the attached safety hardware unit (11) is implemented
diverse.

20. A Control System according to claim 19, **characterized**
in that the attached safety hardware unit (11) is diverse
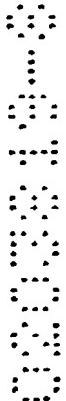generating a safety related header for the bus (14)
communication.

5

ABSTRACT

A Controller is capable of executing non-safety related control logic. A safety module is added to the Controller in order to increase the safety integrity level of a
5   Control System. The Controller is then able to execute safety related control of real world objects. Such a Control System may for instance exist at an off-shore production platform or in an hazardous area of a chemical plant.

10

Fig. 1

15

1/2

Fig. 1

Fig. 2

2/2

Fig. 3

Fig. 4